REMARKS

The foregoing Amendment and the following Remarks are submitted in response to the Office Action issued on April 20, 2005 in connection with the above-identified patent application, and are being filed within the three-month shortened statutory period set for a response by the Office Action.

Claims 15-18, 20-27, 31-34, and 36-43 are pending in the present application. Claims 1-14, 28-30, and 44-46 have been canceled, claims 15 and 31 have been amended to include the subject matter of claims 19 and 35, respectively, claims 19 and 35 have thus been canceled, and claims 20 and 36 have been amended to adjust dependencies. Applicants respectfully submit that no new matter has been added to the application by the Amendment.

As was previously pointed out, the present invention is directed toward the problem that for a computing device such as a portable computing device to be trusted in the context of a rights management architecture, the portable device and the processor thereon must be of a type that substantially completely prevents a content thief from performing nefarious acts that would allow obtaining of content therein in an unencrypted form or decryption keys. Thus, according to the present invention, the processor is a secure processor and is constructed to run only authorized code, and is operated to maintain a strict cryptographic separation between applications that may be instantiated thereon.

The secure processor is operable in a normal mode and a preferred mode, where the security kernel can access a locally accessible CPU key only during the preferred mode. The security kernel employs the accessed CPU key during the preferred mode to instantiate and/or authenticate a secure application such as a rights management system, a banking / financial system, etc. on the portable device. The security kernel may

automatically instantiate a particular secure application, may authenticate a secure application instantiated by another process, or may initially instantiate a secure chooser application that allows a user to select from one or more available secure applications on the portable device.

In any case, the accessed CPU key is typically a symmetric key that is employed by the security kernel to decrypt one or more encrypted security keys for the application instantiated. For example, in the case where the security kernel instantiates / authenticates a rights management system on the portable device, it may be that at least the private key (PR) for the rights management system is already encrypted according to the CPU key and stored on the portable device as CPU(PR), and the security kernel during the preferred mode employs the accessed CPU key to decrypt CPU(PR) to produce (PR) such that (PR) is available to the instantiated rights management system. Thus, the CPU key as accessible only by the security kernel and only during the preferred mode is the key to unlocking or decrypting the secrets identified with each application, and therefore must be well-protected.

The Examiner has rejected claims 15-18, 20-27, 31-34, and 36-43 under 35 USC § 102(e) as being anticipated by Vu et al. (U.S. Patent No. 6,557,104). Applicants respectfully traverse the § 102(e) rejection of such claims.

Independent claim 15 of the present application recites a method for a secure processor to instantiate and authenticate a secure application thereon by way of a security kernel. In the method, the secure processor enters a preferred mode where a security key of the processor is accessible and instantiates and runs a security kernel. Thereafter, the security kernel accesses the security key and applies same to decrypt at least one encrypted key for the application, stores the decrypted key(s) in a location where the application will expect the

key(s) to be found, and authenticates the application on the processor. The secure processor then enters a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible. Thus, the security kernel allows the processor to be trusted to keep hidden the key(s) of the application.

As amended, claim 15 also recites that the security kernel employs the accessed security key during the preferred mode to authenticate / verify the application prior to instantiation thereof.

Independent claim 31 as amended recites the subject matter of claim 15 as amended, albeit in the form of a computer-readable medium.

The Vu reference discloses a secure processor where, during run-time, an application requiring access to a secure service invokes a security routine that in turn invokes a security mode by way of a high-level security interrupt which cannot be otherwise invoked. As best set forth at column 5, lines 24-41, once in the security mode, a security function is invoked to access secrets and data from an otherwise inaccessible storage location, and the security function performs appropriate security functionality based on such secrets and data, such as for example encryption and decryption, password validation, user authentication, etc.

However, and significantly, the Vu reference does not disclose that the Vu security processor instantiates and authenticates a secure application, as is require by claims 15 and 31. Instead, the Vu reference requires that an application already be instantiated so as to invoke and gain access to the security services provided by the Vu security processor. Correspondingly, the Vu security processor reference is not disclosed as authenticating any application on the processor; as is required by claims 15 and 31. At most, the Vu reference discloses user authentication, but not authentication of any application, let alone an

application that is to be instantiated. Likewise, inasmuch as the Vu reference discloses processing security-related requests from an application that is already instantiated, such Vu security processor does not employ any accessed security key during a preferred mode to authenticate / verify any application prior to instantiation thereof, as is required by claims 15 and 31.

To summarize, then, the present invention as recited in claims 15 and 31 et seq. requires that a secure processor be operable in a normal mode and a preferred mode, where a security kernel can access a locally accessible CPU key only during the preferred mode and employ the accessed CPU key during the preferred mode to instantiate and/or authenticate a secure application such as a rights management system, a banking / financial system, etc. on the portable device. Thus, the secure application can be trusted to be authorized code that will not attempt to gain access to secrets maintained in connection with other secure applications on the secure processor, and strict cryptographic separation is thus maintained between applications instantiated on the secure processor. In contrast, the Vu secure processor merely provides security services for already-instantiated applications, and cannot ensure that such applications should in fact be trusted to handle secrets and other secure data appropriately.

Accordingly, Applicants respectfully submit that the Vu reference does not anticipate or even suggest the invention recited in claims 15 and 31 or any claims depending therefrom.

Independent claim 25 recites a method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel. In the method, a chooser value is set to a value corresponding to a chooser application upon power-

up, and a preferred mode is entered upon a power-up CPU reset and instantiating the security kernel. The security kernel determines that the chooser value corresponds to the chooser application and therefore authenticates and instantiates same.

After the chooser application is instantiated, a normal mode is entered and the chooser application presents the plurality of available applications for selection by a user. Upon receiving a selection of one of the presented applications to be instantiated, the chooser value is set to a value corresponding to the selected application. Thereafter, a CPU reset is executed and the preferred mode is entered, and the security kernel is instantiated. The security kernel then determines that the chooser value corresponds to the selected application and therefore authenticates and instantiates same. Normal mode is then entered after the selected application is instantiated and run. Thus, the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application.

Although the Examiner argues that the Vu reference discloses the chooser application, the chooser value, and the use thereof as recited in claims 25 and 41, Applicants must disagree, and in fact respectfully submit that the Vu reference is utterly silent about employing such items to securely choose and instantiate one of a plurality of applications on a secure processor in the manner recited in claims 25 and 41. In particular, the Vu reference does not at all disclose or even suggest switching between modes as recited to first load and then operate a chooser application, employ same to select a chooser value corresponding to a chosen application, and then load and operate a chosen application in the manner recited in claims 25 and 41.

Thus, Applicants respectfully submit that the Vu reference does not disclose or suggest the subject matter recited in independent claims 25 and 41 or any claims depending therefrom. Accordingly, and for all the aforementioned reasons, Applicants respectfully request reconsideration and withdrawal of the § 102(e) rejection.

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 15-18, 20-27, 31-34, and 36-43, is in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

Date: July 11, 2005

Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439